OFFICE OF ACQUISITIONS
NATIONAL CANCER INSTITUTE

REQUEST FOR PROPOSAL NUMBER: N01-PC-55049-40, entitled Cancer Genetics Network(CGN)

Amendment No. 1

Date of Issuance: November 4, 2005

The above numbered Request For Proposal (RFP) is amended as set forth below. The hour and date specified for receipt of Offerors **is changed to Tuesday, December 20, 2005 at 3:00 P.M. Local Time.**

Offerors MUST acknowledge receipt of the amendment prior to the hour and the date specified in the solicitation or as amended, by separate letter, telegram, or Electronic Mail which includes a reference to the RFP and Amendment number(s). For your convenience, the Proposal Intent Response Form is provided in SECTION J - List of Attachments of this RFP, for this purpose.

FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERORS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER.

This Amendment revises the RFP as stated below:

This amendment shall serve to extend the proposal due date and provide clarification/responses to questions posed. **The due date is changed to Tuesday, December 20, 2005, at 3:00 p.m. local time, for submission of proposals**.

Clarification/responses are provided as follows:

Question 1:
Please give guidance on the budget limit. The announcement of the RFP on fbo.gov indicated $6 million, but it was unclear if this refers to direct or total, for the contract only or contract and all subcontracts etc. Similarly, Page 31 of the Solicitation indicated 4,480 hours labor per year, but it is unclear if this is only the DCC or DCC plus all site subcontracts.

Answer 1:
The budget estimate is not public information; therefore it cannot be released. The $6 million listed in the announcement of the RFP on fbo.gov has no association with the budget estimate. It is only to classify the offerors establishment by the type of activity in which they are engaged (ie. Small Business set-aside). All offerors are to submit their proposed budget to NCI.

On page 31 of the Solicitation, 4,480 hours labor per year are for the Data Coordination Center (DCC) only.

Question 2:
Please give guidance on the requirement of CGN subject access. Page 1 of the SOW indicates "offerors and their subcontractors must already have IRB approval to access (re-contact) CGN enrollees and/or their data. This is a critical requirement for proposals for this RFP." Currently, the way the CGN subjects were consented, only the sites and subsites (the future sub-contractors to the DCC) have the approval to contact the subjects. Please clarify what this sentence means to the applicants for the DCC contract.

Answer 2:
Page 1, paragraph 3, of the Statement of Work is changed to read as follows:

> The NCI wishes to maintain the integrity of the CGN enrollee pool as well as the functions performed by the CGN which maintain that enrollee pool and its annual follow-up. Maintaining the CGN database will permit investigators to obtain access to existing data and biospecimens for use in cancer research studies and provide interested investigators information about and access to CGN study enrollees for studies/trials. Therefore, this funding mechanism is being issued to meet the anticipated requirements of the CGN.
>
> Subcontractors must already have IRB approval to access (re-contact) CGN enrollees and/or their data. The Offeror must have permission from the Subcontractors' IRBs or there must be language in the Subcontractor's informed consent forms or there must be other assurances from the Subcontractor Principal Investigator that the Offeror will be permitted to have access to de-identified individual-level CGN data from the Subcontractors.

Question 3:
Please clarify the acceptable methods of obtaining annual follow-up from sites: Page 7 last paragraph (numbered e) of the SOW indicates that centers must use either fax/scan forms or web-based system. If the sites indicate that it is more efficient for them to submit bulk data at regular intervals as they currently do, is that acceptable?

Answer 3:
The Centers must use either fax/scan forms or web-based system. It is the Offerors option to propose batching or not and the frequency of transmission of the information. However, all centers must have the infrastructure for and demonstrate ability to send patient data within 24 hours of obtaining it if needed for a particular study.

Question 4:

Personnel at the subcontracting sites: Page 59 3d indicate that sub-contracting sites should be PI, MD with clinical studies, and data manager. Is this meant to be 3 people or is this indicating that the PI must be an MD?

Answer 4:
Page 59, 3c and d is changed to read as follows:

> c. Qualifications of the Offeror's Key Personnel, which shall include in aggregate a biostatistician or an epidemiologist, an information technology expert, a physician to serve as the medically responsible individual for clinical studies, and a data manager.

d. Qualifications of the Sub-contracting Centers Key personnel which shall include in aggregate the Center's Principal Investigator, a physician to serve as the medically responsible individual for clinical studies, and a data manager.

Note: Composition of the staffing is to be determined by the offeror, provided they can demonstrate how that composition satisfies the requirements of the RFP. The physician is needed so that there is a qualified person to address any medical issue. The Principal Investigator is not required to be an MD.

Question 5:
Conference call for Contracting Officer and CGN sites: Would you be willing to join a call that included all CGN subcontracting sites to answer their questions about the RFP? Can this be held this Thurs Oct 27 in the afternoon? Is 1 pm EDT acceptable?

Answer 5:
As stated in the synopsis, this acquisition is for "Full and Open Competition" and my meeting with the subcontracting sites would not be appropriate at this time. Individual questions should be addressed to the Contracting Officer and responses will be provided through an Amendment to the RFP.

Question 6:
It seems that certain potential contractors (mainly Universities) already have some kind of IRB requirement. See the first page of the statement of work at the end of Section A. Does that mean Abt Associates is ineligible to bid on this?

Answer 6:
As referenced in Answer 2 above "The Offeror is not required to have its own IRB approval or exemption in place at the time of the offer, but must have an IRB approval or exemption in place after Award, if successful, prior to accessing Subcontractor data".

Question 7:
The mandatory qualification criteria in Section M page 56 requires that the Offeror either: 1) obtain a statement of approval from the IRB Chairperson of the subcontracting Center that the Offeror can access and receive data, or 2) provide copies of consent forms demonstrating that access and receipt of data are permitted.

Since this requirement necessarily requires the cooperation from all the members of the network to provide the requested materials, it defacto prohibits the participation of offerors from outside the network absent such voluntary cooperation.

Answer 7:
See Answer 2 above. The requirement has been modified and does not now have a requirement that the Offeror have an IRB in place that permits access to the data from the potential Subcontractors. In addition, the requirement permits other forms of assurances from the Subcontractors to the Offerors that access to the data would be provided to the Offeror.

Question 8:
Is it the intent of NCI to limit the competition to within the existing CGN Network members?

If not, what action will NCI take to make this RFP truly a full and open competition?
a). Drop the mandatory requirement;
b). Make available to all Offerors the Centers' consent forms;
c). Make available to all Offerors the statements from the IRB Chairpersons of the subcontracting Centers?

Answer 8:
It is not NCI's intent to restrict competition to the network members; however, offerors must demonstrate how they can meet the mandatory qualification criteria.

Question 9:
Will the NCI still fund the Data Coordinating Center if only some of the subcontracting centers can meet the mandatory requirement?

Answer 9:
Page 58, Item 1.b. is changed to read as follows:

b. Technical Approach for maximizing the number of participating centers. *Task 11*

Question 10:

Is the section "Technical Proposal Instructions" the only place where we need to write something regarding our statement of work? When you say "offeror" does it mean the subcontractors or the IT institutions?

Answer 10:
The Technical Proposal Instructions outline what is required in your Technical Proposal including your approach to the Statement of Work. The Offeror is the institution proposing to perform as the Data Coordinating Center.

Question 11:

As a subcontractor, can we ask to review the final proposal submitted by the offerors.

Answer 11:
You may not ask to review the final proposal submitted by the Offerors. The only information you would be privy to would be that of the Offeror with whom you are proposing to subcontract, at his/her discretion.

Question 12:
Our informatics staff is trying to access the Security Plan Outline (pg 16 of RFP) and is unable to access the document. Is there another way to access this on-line? Or can someone email/fax it to us?

Answer 12:
This site is restricted to NCI users only. The Security Plan Outline is included as an Attachment to this Amendment.

NCI edits to the RFP are as follows:

Edit 1:
Page 57, the following subcontracting center is added:

University of California at Irvine - Subcontracting Center

Edit 2:
Page 57, the University of Texas, San Antonio, TX is modified to read:

University of Texas, San Antonio (San Antonio Research Institute)

Edit 3:
A Cancer Genetics Network Investigators Contact Information Roster for the Subcontracting Centers listed in the RFP is included as an Attachment to this Amendment.

Edit 4:

A Literature Article that describes a Cancer Genetics Network Center is included as an Attachment to this Amendment.

Edit 5
Page 16, Item d. System Security Plan, and item e. Rules of Behavior are revised as follows:

(d) Systems Security Plan - is revised to delete in its entirety the two web addresses listed. The Security Plan Outline is included as an Attachment to this Amendment.

(e) Rules of Behavior - is revised to delete the following web address in its entirety:

http://intranet.hhs.gov/infoesc/docs/policies guides/ISPPH/PG ISHbkv2 11 12 2004.pdf

AND

The web address at http://irm/cit.nih.gov/security/nihitrob.html is to be used to access Rules of Behavior.

NIH Information Technology General Rules of Behavior

Introduction

What is the Purpose of The Rules of Behavior?

The intent of these NIH Rules of Behavior are to summarize laws and guidelines from various NIH and other Federal documents, most specifically OMB Circular A-130. These guidelines should be used by all ICs as a basis for their own security plans.

What are Rules of Behavior?

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

Who is Covered by These Rules?

These rules extend to all NIH personnel and any other persons using IT equipment or accessing NIH systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, NIH's security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and NIH Records Management Regulations.

What are the penalties for Non-compliance?

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of

system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. NIH will enforce the use of penalties against any user who willfully violates any NIH or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the NIH published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

Accountability-General Requirements

Users:

- Users should adhere to the DHHS Standards of Conduct and behave in an ethical, proficient, informed, and trustworthy manner.
- Do not attempt to override technical or management controls (i.e., carrying sensitive data home on a floppy disk without prior approval, etc.).
- All users should complete the NIH Computer Security Awareness Training prior to obtaining access to NIH systems.
- Use virus protection software.
- Use only systems, software, and data for which you have authorization and use them only for official government business, or in accordance with the NIH Personal Use policy located at http://www3.od.nih.gov/oma/manualchapters/management/2806/.
- Report security incidents, or any incidents of suspected fraud, waste or misuse of NIH systems to appropriate officials.
- Encrypt sensitive information when reasonable and worthwhile.
- Protect passwords from access by other individuals.
- Change passwords frequently. The frequency should be commensurate with the risk and criticality of the system, but should be no less often than every six months. The current NIH Password Policy can be found at http://irm.cit.nih.gov/policy/passwords.html.
- Protect confidential and/or sensitive information from disclosure.
- Protect government property from theft, destruction, or misuse.
- Do not remove computers from NIH premises unless authorized in accordance with NIH property management requirements.

Managers:

- Ensure that staff are given access to, and ample time to complete, the NIH Computer Security Awareness Training.
- Ensure that staff has access to, and are aware of, all existing NIH and federal policies and procedures relevant to the use of NIH information technology resources.
- Ensure that staff follows system security policies, guidelines and procedures.

Remote Access Off-site Use of IT Resources

- Use government resources for authorized purposes only, or in accordance with the NIH Personal Use policy located at http://www3.od.nih.gov/oma/manualchapters/management/2806/.
- Take precautions to secure government information and information resources.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Use only authorized, licensed NIH software on government equipment unless authorized to do so according to the NIH Personal Use Policy.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up-to-date.
- Access sensitive information over the Internet only with prior approval from the IC ISSO or appropriate management official.
- Change passwords frequently.
- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.

NIH guidance on remote access security can be found at http://irm.cit.nih.gov/security/SecGui.html.

Appropriate Use of the Internet and E-mail

- Refer to the Guidelines for Appropriate Use of the World Wide Web by NIH Employees at http://irm.cit.nih.gov/policy/guideli2.html.
- Use the Internet for business purposes only when on official government time, or in accordance with the NIH Personal Use policy located at http://www3.od.nih.gov/oma/manualchapters/management/2806/.
- Be aware when navigating through the Internet; you may be moving from an area of controlled access into an area of unknown security controls.
- Report any security incidents to the appropriate officials.
- Do NOT send highly sensitive information via e-mail or fax, unless encrypted.
- Refer to http://oma.od.nih.gov/ms/records/rmanagement.html for the latest guidance on records requirements for official e-mail records and facsimile documents, or contact your IC Records Management Officer.
- Protect copyrighted software and information in accordance with the conditions under which it is provided.
- All Contractor staff who have access to and use NIH e-mail must set up an Autosignature or electronic business card (v-card) on their computer and/or personal digital assistant (PDA) to visibly identify themselves as a contractor on all outgoing e-mail messages, including those that are sent in reply and on messages that are forwarded to another user. For more information, see "New Requirements for NIH Contractor" Designations in Email located at http://irm.cit.nih.gov/policy/contractors.html

Access Control

Users:

- Grant access to systems and data only to those who have an official need to know.
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- Never share or compromise your password.
- Make alternative provisions for access to information during your absence to avoid the sharing of passwords.
- Include the following disclaimer on the fax cover sheet when sending faxes:

  ******WARNING******

  The attached information may be confidential. It is intended only for the addressee(s) identified above. If you are not the addressee(s), or an employee or agent of the addressee(s), please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this fax in error, please destroy the document and notify the sender of the error. Thank you.

Managers:

- Delete or reassign accounts as soon as users no longer require access.
- Plan for disaster recovery and contingency situations.
- Determine access levels based on the user's duties and need to know.

Information Technology (IT) service providers:

IT service providers include (but are not limited to): system administrators, computer operators, system engineers, network administrators, LAN server administrators, those who have access to change control parameters for equipment and software, database administrators, those who control user passwords and access levels, and troubleshooters/system maintenance personnel. IT service providers must:

- Restrict system access to those persons needed to perform assigned duties.
- Ensure system users are aware of their responsibilities regarding access security.
- Plan for disaster recovery and contingency situations.
- Be certain proper software access controls are in place to ensure the security and integrity of data.
- Post logon warning banners at all logon points to Government computers and systems where technically practical. The banner policy and an example can be found at http://irm.cit.nih.gov/policy/warnbanners.html.
- Set passwords for new accounts.
- Set expiration dates for accounts and passwords (passwords must be changed at least once every six months).
- Delete or reassign accounts as soon as users leave NIH.

Selecting Passwords:

The objective when choosing a password is to make it as difficult as possible for a cracker to make

educated guesses about what you've chosen. This leaves him/her no alternative but a brute force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try millions of passwords per second, would require many years to complete.

What Not to Use

- Don't use your login name, e.g., smithj, in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

What to Use

- Do use a password with mixed-case alphabetics if system password is case-sensitive.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation or combine with alphabetic characters, e.g., $robot2!
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Information Management

General Rules:

- Place only mission-oriented information on a public access system, including Internet Web pages, e-mail servers, and news groups.
- Ensure that appropriate management officials have approved information for public dissemination.
- Ensure that you do not disclose any sensitive or inappropriate information through the use of public access connections.
- When providing a Web page, a disclaimer should be displayed on the home page, or linked to on the Internet or Intranet. More information can be found at http://irm.cit.nih.gov/policy/guideli2.html.
- Persistent cookies or fill-in forms should never be used on a site to collect data from users unless pre-approved.
- Ensure that sensitive information sent to a fax or printer is handled in a secure manner, e.g., cover sheet to contain statement that information being faxed is confidential.

- Ensure electronic official records (including attachments) are printed and stored according to NARA's guidelines. Contact your IC Records Management Officer http://oma.od.nih.gov/about/contact/browse.asp?fa_id=2.

Backing up Systems:

- Backups should be performed commensurate with the risk and criticality of the data.
- Ensure backups are successful and copies are kept off site.
- Ensure data can be easily restored when necessary.
- Ensure virus protection software is in use and is current.
- Follow up on reported security incidents in a timely manner.
- Destroy backups when no longer needed.

Disposition of Sensitive Resources:

- Hard copies of highly sensitive information should be destroyed by pulping or shredding.
- Highly sensitive information stored on removable media should be entirely erased, or the disks destroyed. When disposing of, or transferring a computer system, erase all files from the hard drive by using a wipe out utility, or destroy the disk if necessary according to the NIH Records Management Guidelines. Please refer to the following URL for the current NIH Sanitization policy: http://irm.cit.nih.gov/security/sanitization.html.

Date published: 03/21/02
